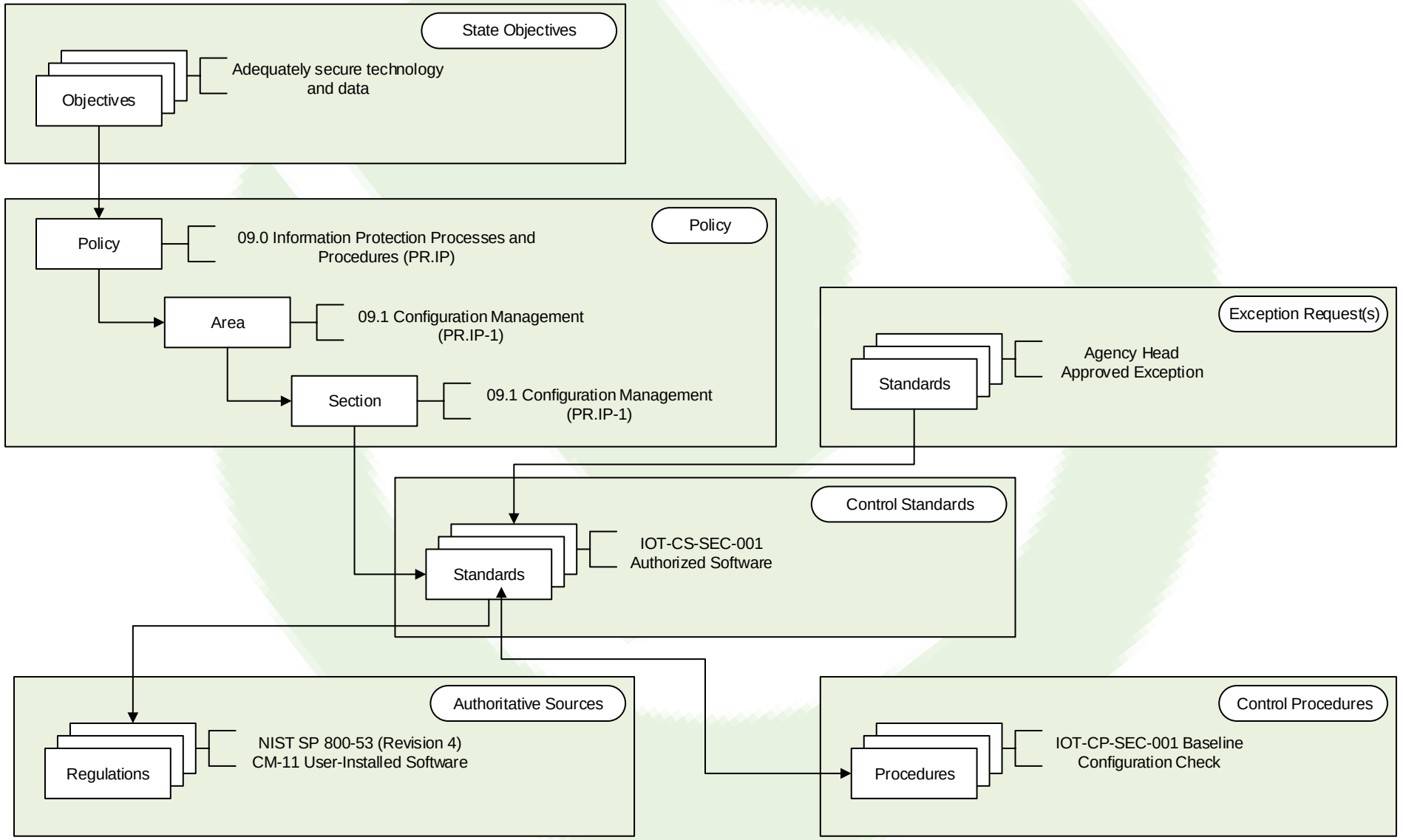
Indiana Office of Technology

Powering a State that Works

Policy Management

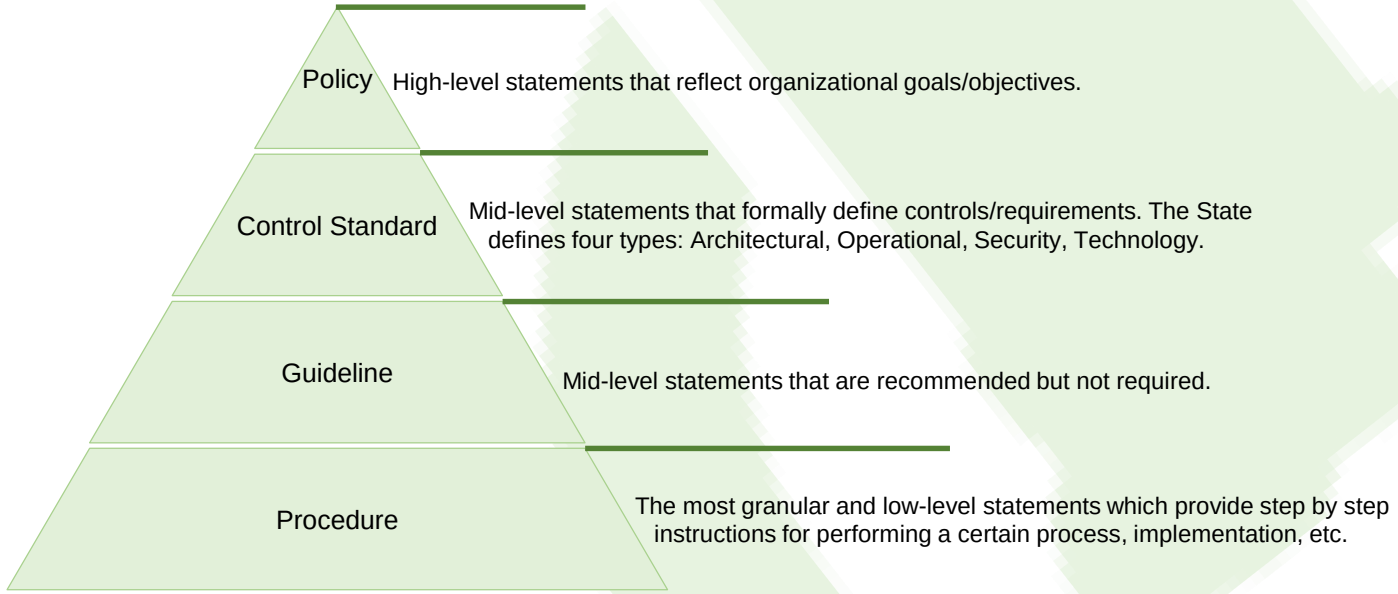
Bryan Sacks, Director of Risk & Compliance

Policy Management Structure (Big Picture)



Policy Management Terminology and Structure

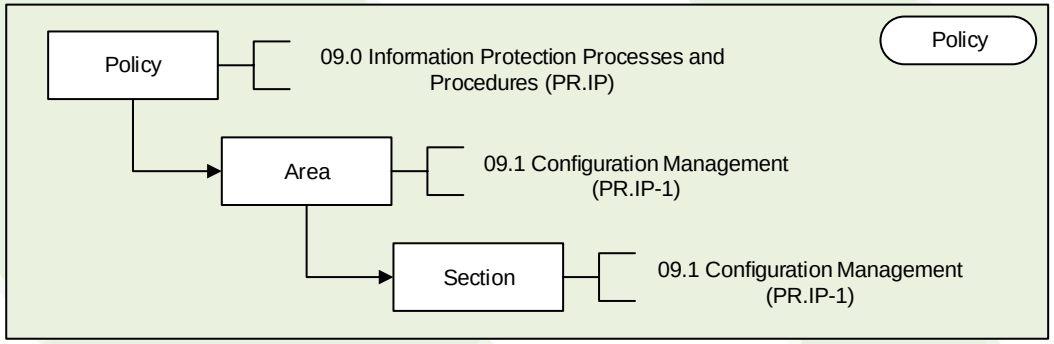
There are many different interpretations of what Policies, Standards, Guidelines, Procedures, etc. are and how they should be written. A common understanding and one that the State follows is represented by the graphic below:



As the State moves towards implementing this approach, this framework will be used in the State's Governance, Risk and Compliance (GRC) tool, Archer. The following slides will break-down the each level and display the interconnections between some of the components.

Policy

The Policy structure in the State's GRC tool is hierarchical down to specific subcategories called Area's and Sections. Below is a pictorial view:



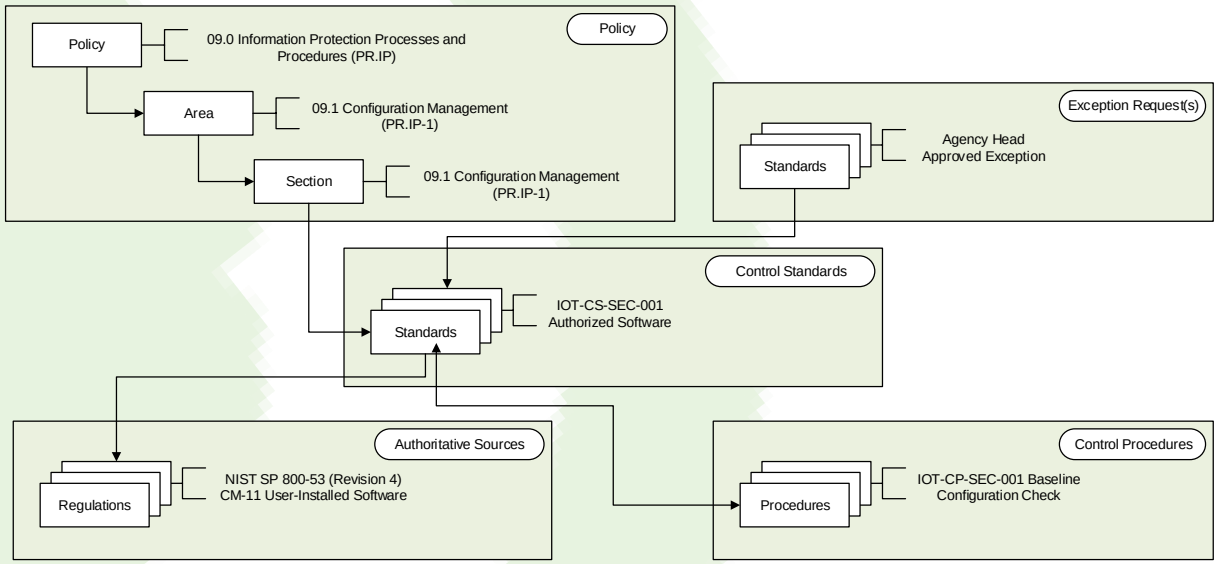
Policies align to the 22 Categories described in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and both Area and Sections align to the 98 Subcategories described in the NIST CSF. Due to the configuration of the tool, it is necessary to have the same Area and Sections, as Control Standards can only be mapped to Sections. As NIST continues to update guidance, it is possible that this structure may be modified to best fit the needs of the State.

Control Standards (1/2)

The Control Standards are the core of the Policy Structure. As you can see through the pictorial view below, Control Standards map to Policy Sections, Authoritative Sources and Control Procedures.

Control Standard

Mid-level statements that formally define controls/requirements. The State defines four types: Architectural, Operational, Security, Technology.



Security Control Standards are aligned with the NIST Special Publication (SP) 800-53 Revision 4 controls. There is alignment across other Authoritative Sources such as HIPAA and PCI. Control Procedures should not be confused with ‘Procedures’ or ‘Operating Procedures,’ they are a mechanism to test against the compliance of a corresponding Control Standard. Procedures or Operating Procedures refer to day-to-day items or implementation, not to control testing.

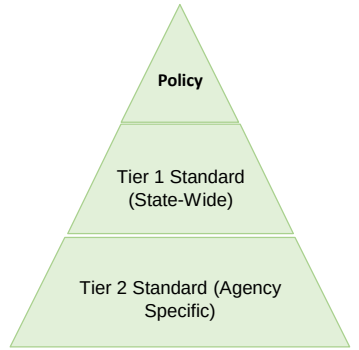
Control Standards (2/2)

Control Standards follow a hierarchical approach and have multiple types. A hierarchy is required as agencies may wish to implement Control Standards that are more stringent than the State's requirements, set by IOT.

1. Hierarchy
    1. Tier 1 – Control Standards written by IOT for the enterprise, all agencies are required to demonstrate compliance and file exceptions (when allowed) against Control Standards.
    2. Tier 2 – Control Standards written by Agencies that meet or enhance Control Standards written at the Tier 1 level.

2. Types – There are multiple types of Control Standards that can be written, below are the four defined in the State environment:
    1. Architectural – established by IOT architects as required configurations (e.g., how confidential applications must be configured)
    2. Operational – established by IOT service delivery teams as requirements for day-to-day items (e.g., email retention)
    3. Security – established by the IOT security team as requirements for controls related to identifying, protecting, detecting, responding and recovering from information security related items
    4. Technology – established by IOT service delivery teams as requirements for standardized technology (e.g., available laptop choices)

Hierarchy:



Types: